# St Paul's College Netbook/ Computer Acceptable Use Policy

## St Paul's College, Kempsey

2016

## Table of Contents

**Scope and Purpose Section A** ..... **1**
**Policy Outlines** ..... **1**
**Terms and Conditions** .....
**Students** ..... **2**
**Teachers** ..... **3**

**Advice and Management Section B** .....
**Internet and Email** ..... **4**
**Computer storage devices** ..... **6**
**Consequences of misuse** ..... **8**
**Social media advice** ..... **9**

**Letters, plans and material Section C** .....
**Sources and website advice** ..... **10**
**Example letter home** ..... **11**
**Computer work plans sheet** ..... **12**
**Policy authority agreement sheet** ..... **14**

## Scope and Purpose Section A

### Overview

At St Paul's College, we allow all students access to our computer network, enabling them to use standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the Internet and electronic mail. Every student is issued with a username, password and an email address at the start of their schooling career.

Access to the computer network is a privilege and it is the students' responsibility to restrict themselves to usage which is ethical and appropriate. Failure to comply with the rules which govern the use of the network may result in consequences being administered to the student. These consequences will be in keeping with the College Discipline Policy, and may require referral to the Year Coordinator and/or Assistant Principal. These consequences may include loss of access privileges, or in serious cases, suspension or review of enrolment. Parents will be informed when serious breaches of the Acceptable Use Policy have occurred. Further legal action will be carried out if deemed necessary.

Students are encouraged to make use of IT facilities in support of their studies in all subjects, including the writing up of coursework assignments and other projects.

The College provides a network environment in which students can assume that their legitimate use of computers and the data that they store are secure against interference by other users. Students should not, however, assume that their activities are completely private. The College retains the right to determine appropriate use and to monitor user accounts, and fileserver space as judged necessary. Hence, records of usage, files that have been stored, and email messages that have been sent or received, and external memory devices, SD cards and devices of that nature may be scrutinised by the members of staff responsible for management of the network either (a) during routine system maintenance, or (b) if there is reason to suspect misuse of the network or the device.

St Paul's College makes no warranties of any kind, whether expressed or implied, for the service it is providing. St Paul's College will not be responsible for any damages, including the loss of data.

St Paul's College may update this AUP at any time.

## Policy Outlines

### 1. Policy Purpose

Computing devices and network access are provided to students to enhance teaching and learning. The use of these devices and services requires informed parental consent and appropriate management.

### 2. Background

Students, teachers and other St Paul's College community members need to have clear guidelines to ensure that information technology resources are used appropriately. These guidelines will assist teachers at St Paul's College implement procedures that both protect and educate the students in their care.

### 3. Definitions

Computing Device – Includes Desktop computers, laptop computers, netbook computers, tablet computers and other devices capable of accessing the College network.

Inappropriate Material – Any material that is offensive, abusive, discriminatory, defamatory, illegal or lewd and lascivious (including, but

not limited to, pornography) is considered inappropriate. If a student is unsure if material is appropriate they should check with their teacher before attempting to access it.

Bullying – Persistent behaviour that causes hurt or distress for another person. Bullying may be "unintended", however the impact on the victim will be considered.

## 4. Access and Security

Access to the College network is carefully monitored and controlled to safeguard student welfare and enhance learning. Users are not to attempt to subvert the College network security systems, including, but not limited to, the College proxy server and installed anti-virus software.

Intentionally subverting these security measures may seriously compromise the safety and security of other users and will result in a loss of access privileges.

Any user who inadvertently discovers a breach of the College's security systems or who witnesses' inappropriate use of the College's network of computing devices is to report the incident immediately.

## 5. Personal Information, Privacy and Confidentiality

College staff have to balance the privacy rights of individuals against their moral and legal obligation to protect students from harm and ensure that any computing resources are used to enhance teaching and learning. As such, teachers will inspect the contents of any computing device provided by the College and/or other personal devices from time to time. Furthermore, access to the Internet and the College network will be monitored and reviewed.

## 6. Intellectual Property and Copyright

All users are expected to only use legal content on their College provided computing device. Using College resources to access illegal or pirated material is strictly prohibited and may result in the matter being referred to the appropriate authorities for serious breaches.

Furthermore, users are to ensure that any work that they submit or host on a College computing device or network is original and appropriately referenced. Plagiarism is a serious academic matter and may lead to disciplinary action.

## 7. Appropriate Use – Terms and Conditions

**Students**:

- agree to adhere to the terms and conditions set out in this Acceptable Use Policy each time they use a computing device provided by the College and/or access the College network.
- will ensure that all communication using the computing device provided by the College and/or separate online services is related to learning or school activities
- will keep passwords confidential, and change them when prompted or when known by another user
- will never knowingly allow others to use their computing device or network account unless directed to by a teacher for the purposes of collaborative learning
- will not send or publish unacceptable or unlawful material or remarks including offensive, abusive, defamatory or discriminatory comments
- will not access or attempt to access inappropriate material
- will not attempt to impersonate any other person when using the College provided computing device or College network

- will not engage in any bullying, intimidation or other inappropriate behaviour online

- will immediately tell a teacher if they receive a computer virus or a message that is inappropriate or makes them feel uncomfortable

- will never knowingly initiate or forward emails containing:

  - ✓ a message that was sent to them privately

  - ✓ a computer virus or attachments that are capable of damaging the recipients' computers

  - ✓ chain letters and hoax emails

  - ✓ "spam", like unsolicited advertising material, or mail unrelated to learning

- will not damage or disable computers, computer systems or networks of the College or other entity

- will not attempt any repairs on the computing device provided by the College, nor open the machine's enclosure in any way.

- will ensure that online services are not used for unauthorised commercial activities, political lobbying, gambling or any unlawful purpose.

- will not attempt to access the College's network using an unapproved private device, including but not limited to, smartphones or games devices

- will ensure that they have an appropriate data backup strategy. For example, all important data (e.g. assignments) should be backed up to an external device every week. Furthermore, important documents should also be stored in a "cloud-based" backup facility like Dropbox (www.dropbox.com).

- will not install software on any College computing device without completing the appropriate Software Installation Request document and receiving the approval of the Learning Technologies Coordinator.

- will promptly comply with all instructions from their teachers relating to the use of College computing devices and network systems.

- will ensure that any computing device is charged at night for use at school the following day.

- will not use any College computing device while travelling to and from the College or between classes. Any computing device must only be transported secured inside an appropriately padded bag.

- will not use any College computing device in the playground at recess or lunch.

- will not use the camera option on any device at school without teacher permission.

### Teachers:

- are responsible for supervising student use of the College provided computing devices and access to the College network.

- are to maintain an informed view of the relative risks and educational benefits of online activity by their students. A variety of resources are available from the Internet sites listed in Section 8 of this policy document.

- are to ensure that students are aware of the possible negative consequences of publishing identifying information online including their own or other students' images

- are to check that any material planned for publication on the Internet or College network has the approval of the Principal and has appropriate copyright and privacy clearance

- are aware of the steps to take and advice to give if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public. Such steps may include:

- ✓ collecting as much information as possible about the incident including copies of communications
- ✓ emphasising to the student that the event is not necessarily their fault
- ✓ identifying any risky behaviours on the part of the reporting student and counseling them on the need to adopt more protective behaviours
- ✓ if the incident warrants further attention inform the Principal of the incident (for example, if the teacher suspects the student may have been placed in a position of harm)

• are to inform parents that student Internet access from home or other non-school sites does not occur via the College's network and therefore Internet browsing may not be filtered

• should promote the use of strong passwords for students who can cope with the complexity. Stronger passwords:

- ✓ contain a mixture of alphabetic and non-alphabetic characters
- ✓ are changed frequently
- ✓ do not contain dictionary words
- ✓ do not contain easily identified personal information such as name, date of birth, etc.
- ✓ do not contain any part of the account identifier such as the username

## Section B- Internet and Email

### INTERNET USERS AGREEMENT

The Board of Studies has mandated that IT is to be studied and as such, access to the Internet must be provided. However, there are standards of behaviour that their children should follow when using media and information sources. Students are responsible for good behaviour on school computer networks just as they are in a classroom or any other school function. Violations may result in a loss of access as well as other disciplinary or legal action.

We regard the use of the Internet to search for and use information related to a College subject as acceptable. The Network is provided for students to conduct research and communicate with others in relation to their work. Therefore, they will not look for material, which is unrelated to school curriculum, unless they have the written permission of a teacher. Every student in the College has access to the Internet and has a College email account. The email account is only to be used for educational or school related purposes. It is not be used for private email communication.

### 2. Rules

When using these facilities, students are expected to behave with normal standards of courtesy, and within the guidelines of the expectations, which St Paul's College has of the students enrolled in it.

#### a. General 'Netiquette' Net Etiquette

Students must not:

- Send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
- Disclose to a third party the personal details of any other student.
- Access any inappropriate Internet site, or attempt to access offensive or inappropriate information.
- Breach another person's copyright in any material, therefore the St Paul's College Guidelines in relation to plagiarism must be followed.
- Download any material from the Internet unless instructed by your teacher.
- Send a network message

- Join any List Serve email services unless approved by a teacher
- Cause any unsolicited email to be sent to another person's email address
- Send a message with someone else's name or a false name.
- Send a message that is inconsistent with the College's code of conduct and standards.
- Send a personal email during lesson time that is of a private nature or unrelated to schoolwork.
- Upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
- Purchase goods or services via the computer network, or use the Network for commercial gain.
- Use the computer network to gain unauthorised access to any other computer network.
- Attempt to spread computer viruses.
- Bring to College via any device or email, any games or other software or any material that is inappropriate or offensive.
- Open all email attachments before saving them to allow virus scanning before being opened.
- Plug in any device to College computers other than a simple USB memory stick, or a memory stick approved specifically by the IT teacher.
- Engage in any activities that contravene the St Paul's College Student Expectations.
- Engage in activities that are prohibited under Australian Law. Thus the transmission of material subject to copyright or Australian Law is forbidden, as of course is any threatening or obscene matter.

### b. Personal Safety

In addition, Students need to be aware that thoughtless use of email and the Internet may jeopardise their personal safety either at College or outside College. Students should therefore:

- Never arrange a meeting in person with anyone they have "met" or only communicated with by computer, without prior parental approval.
- Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way. If such a message is encountered the student should report it to his or her teacher and parents.
- Be aware that any person they "meet" or communicate with online may pretend to be someone else.
- Remember that anything they read online may not be accurate, or may misrepresent a person or situation, and thus take care in the use of this information.
- Ignore offers that involve either financial transactions or personal meetings.
- Not disclose any personal details, such as their home address or telephone number, across the Internet.
- Ensure that personal Internet browsing and email use is conducted at home.

## INAPPROPRIATE MATERIAL

Unless required by a particular educational context, the following are to be considered inappropriate or offensive:

- Gambling sites
- Games or game sites
- Nudity
- Sexually explicit or suggestive material
- Material relating to violence

- Material that is discriminatory or offensive to a person's nature or to a particular social group. This can include: physical, intellectual, emotional aspects; religious beliefs; race; gender and gender preference.

- Language that is generally considered obscene or blasphemous.

### USE OF COMPUTER STORAGE DEVICES

The use of multi-functional storage devices such as USB memory sticks, handheld computers/PDAs/iPods/USB keys/mp3 players, etc.

Guidelines on the Use of Computer Storage Devices

- External hard drives are not to be used by students in the junior school, unless the IT teacher has given specific permission for them to do so for a period of time. The only senior students who may use an external hard drive are those who study IT and Industrial technology at school, and who have the specific permission of the IT teacher. The IT teacher will nominate the specific external hard drive to be used on the school network. Other types of external hard drives are not to be used.

- Students are permitted to use the school approved USB/memory sticks/flash if the course teachers require them to do so. However, in using these devices the students are asked to keep in mind their obligation to the school.

- In terms of the security of the College's computer system students are asked to ensure that these devices are free of viruses or any malicious software of any kind.

- Further students must be aware that the school has the right to see the contents on these devices. This may entail that the student hands in the memory stick, or such device, to any teacher who requests it. The memory stick will be kept until the College is satisfied that the contents on it are appropriate.

- Storage devices such as CDs/DVDs and USB memory sticks can be used to store and transfer files to or from College computers.

- Mp3 devices, PDA's, iPods, mobile phones and other storage devices must not be used to transfer files to or from College computers unless supervised by specialist teachers.

- No devices may be used to listen to music, watch videos, send messages or play games within the College, unless the device is provided by the teacher, and the teacher has approved the content. The penalty for this will include confiscation of the device. Other consequences may be applied in keeping with the College's AUP and general rules and expectations.

## Consequences of Computer Misuse

The following are policy consequences for failure to comply with acceptable computer usage in class or at home. The consequences are not final and may be adjusted by the LTC or Principal due to considerations. They provide a basis by which disciplinary matters can be resolved.

List of offenses may include:

- Gaming
- Off topic use of Internet/computer
- Not having computer ready for class (forgetting computer)
- Not having battery charged
- Damage to computers

### Consequences

1. Warning in class – teachers can give warnings in class but a repeat offense of issue can result in:

    a. Turning off computer / restriction of classroom use

b. Sending to LTC

c. Sent to collect computer for lesson if not brought or charged. (subject to supply)

2. For continued misuse or failure to comply with acceptable usage policy's students are to be sent to the LTC. They may incur:

   a. A warning from the LTC

   b. A letter home to parents

   c. Detention

   d. Possible Suspension

3. Further infringement of the policies will incur:

   a. A letter to parents

   b. Possible Suspension

   c. Afternoon detention

   d. Removal of computer take home privileges

   e. Being placed on a computer progress behavioral report with the LTC

- A work plan may include completion of IT progress behavioral form signed by every class teacher for appropriate use of computer. This would be handed in to the LTC with the collection and returning of computer to LTC every day

## Social Media Use Tips for Staff

With more staff using online social media both personally and professionally to learn, advocate, collaborate, exchange and contribute, for the benefit of your professional and personal development, the college is endeavouring to formulate a social media policy. This will give you some guidelines and guidance as to the proper etiquette when engaging with these online tools, for the protection of your personal and professional reputation and that of the college. In the meantime I have sourced the DET social media guidelines, and did a little plagiarism from other policies that you might find helpful.

## General Social Media Use Guidelines

Social media is not about technology but about using it to connect with people, so remember that your conduct reflects not only on yourself but on the college. Social media is blurring the lines between the personal and professional aspects of many people's lives, and anything posted can have an impact on both. Please bear this in mind when posting.

- **Be transparent.**
- **Protect your privacy.**
- **Be accurate.**
- **Be respectful.**
- **Be responsible.**
- **Always think before you post.**
- **.Maintain personal and organisational confidentiality.**
- **Respect College time and resources.**

## When representing St Paul's online

Please be considerate, transparent and understand that as a St Paul's College staff member you are representing your employer and their reputation but we do value your engagement in and positive use of social media on behalf of St Paul's as it is vital we stay relevant and connected.

As well as the general guidelines above, you should also consider the following.

- **Be personable.** Be honest about your identity, and speak in the first person.

Be transparent about being a St Paul's College staff member and why you are posting. If you are posting for publicity or promotional reasons please see Michael first.

- **Be appropriate.** Consider the context in which you're representing St Paul's and choose your tone appropriately based on your audience. Social media means just that – it's about communicating with people so always post smartly, with respect and empathy.
- **Use a disclaimer.** Make it clear this is the content you are authorised to post or the information you have to hand.
- **Be connected.** Wherever possible connect with other St Paul's websites.
- **Be committeed.** Successfully engaging in social media means committing to regularly posting fresh content.
- **Ensure continuity.** Social media requires two way interaction, open dialogue and continuous fresh content. Ensure you not only have a plan for when to begin engaging, but when to handover to other colleagues or areas, and when and how to leave a community, thread or group.
- **Be active and add value.** Make sure you are contributing valuable insights. . For authenticity and credibility, monitor your comments, delete spam and abusive posts, and build your networks and communities in a way that adds value to your online and offline profile.
- **Reference your work.** Always provide links or references when posting content. Don't breach copyright laws, abide by creative commons licences, and obtain consent when citing colleagues or organisational links when reposting content.
- **Think about your customers.** Remember you're not just communicating your also providing customer service. Be personable, relaxed and friendly, as appropriate to the channel or site you're communicating on.

## Use of recording devices by Student or teachers

### Definitions

**Recording devices:** Any camera that can record images be they photo or Video. This includes phones, iPads, computers or any other.

Any device that can also record audio.

**Student**

**Students are not allowed to record any imagery or Audio on school ground without permission of a teacher or the school.**

**Teachers may use recording devices for the following reasons:**

- Teacher Training
- Educational instruction
- Child protection
- Classroom Management
- Student projects under supervision

***Source:***

*Curtin University Social Media Policy*

## Website Sources and Advice

Source:

Curtin University Social Media Policy

Online resources for Appropriate Usage and Cyber-Safety

http://www.cybersmart.gov.au/

http://www.

# St. Paul's College

PO Box 145, West Kempsey, NSW 2440

Telephone (02) 6562-7200

Fax: (02) 6563-1364

Email: spckemp@lism.catholic.edu.au


Date: ……..

Dear Parent / Guardian,

It has come to our attention that …….has been using their College Netbook/iPad to access inappropriate content, namely:

……

……

……

……

We would ask you to remind your son or daughter that accessing, or attempting to access, inappropriate material is in breach of the Acceptable Use Policy. Further breaches may result in a loss of access privileges.

Thank you for your support in this matter.

Yours sincerely,

James Westman ……

Learning Technologies Coordinator Teacher

---

***Please tear off this bottom portion and return to the College***.

I have received the Acceptable Use Policy breach notification dated …….. for

……

I would / would not like you to contact me to discuss the matter.

Parent / Guardian Name: …… Date: ……

# St. Paul's College

IT Computer/iPad Use Progress and Behavioural Report

Student: _____

Year: _____

Date: _____

Teachers the student requires you to fill out this form and sign each lesson. The student is to show me at the start of each day and return the sheet to me at the end of the week. If you have any issues/concerns please make a comment and see me if needed.

Mr Westman

Day 1

| **Subject** | **Teacher** | **Computer Ready for Class Yes/No** | **Appropriate Use of Computer Yes/No** | **Teacher Comment** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Day 2

| **Subject** | **Teacher** | **Computer Ready for Class Yes/No** | **Appropriate Use of Computer Yes/No** | **Teacher Comment** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# St. Paul's College

Progress and Behavioural Report

Day 3

| Subject | Teacher | Computer/iPad Ready for Class Yes/No | Appropriate Use of Computer Yes/No | Teacher Comment |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Day 4

| Subject | Teacher | Computer/iPad Ready for Class Yes/No | Appropriate Use of Computer Yes/No | Teacher Comment |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Day 5

| Subject | Teacher | Computer/iPad Ready for Class Yes/No | Appropriate Use of Computer Yes/No | Teacher Comment |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

ST PAULS COLLEGE KEMPSEY

iPad and Policies Manual

# iPad User Guide

ST PAULS COLLEGE KEMPSEY

# iPad User Guide

---

Mr Westman
St Paul's College Kempsey
Phone 02 65627200 • Fax 02 65631364

# Table of Contents

## Contents


St Paul's College: iPad Pledge ..... 12
Some benefits of using an iPad ..... 2
Issues and how to handle them ..... 2
How to apply restrictions ..... 3
    How to turn on parental controls for the iPad ..... 3
Getting started and setting up an account ..... 5
Redemption codes example sheet ..... 5
Computer Policy Handbook ..... 6
Remember ..... 6
APPENDIX ..... 7

## Some benefits of using an iPad

1. Saving money by combining books, diaries, writing implements, calculators, word processors, etc. all in one media tablet.
2. Allowing students to take control of their own learning.
3. The touch-screen interface allows students to engage more interactively with content.
4. Education programs can be tailor made for each student.
5. Wi-Fi and 3/4G connectivity allow for almost instantaneous and continuous access of information. The ability to quickly switch between applications makes it easier for students to switch between different modes of learning (i.e. research and creation).
6. Mobile data collection is generally streamlined and easy.
7. The iPad easily integrates with existing IT systems. With cloud-based computing, students have connectivity anywhere within the school grounds. There is no need for schools to continue to allocate large budgets for computer power that is no longer necessary.
8. School districts have been creative in finding ways to save money using the iPad. From digital textbooks, to tests and to homework, there's the potential to save huge amounts of money through paperless innovation.
9. iPad's are accessible to students with disabilities. Apps are available for children with cognitive learning problems and there are also accessibility tools built into the latest iOS such as Speak Auto-Text, White on Black, Voice Over and Siri, a voice recognition technology.
10. The iPad can easily be positioned for comfortable use on your desk or lap. Students can also purchase cases and stands which allow devices to be propped up at an appropriate viewing and typing angle.
11. The iPad can also be paired with an external keyboard to ease and speed up typing.
12. There is no delay to boot up iPad's like there is with netbooks or laptops, and no time lost figuring out complex software applications.
13. The iPad's intuitive design and easy-to-use interface makes it simple for even young children to navigate, thereby optimizing the learning experience of all students.
14. The App Store/iTunes Store offers a vast amount of free or low cost apps, many of which are excellent for the classroom.
15. Its light weight and portability means it can easily be carried from class to class without having to close and reopen the screen. Data can be accessed while standing and notes can be taken on the go, thus extending learning far beyond the classroom.
16. It has far less of a strain on children's backs since one iPad replaces a bag full of books.
17. Children are eager to embrace new technology and many are able to troubleshoot computer issues and resolve them quicker than adults.

## Issues and how to handle them

As with all electronic devices, iPad, phones and computers there is a great tendency for students to become distracted by the extra activities that these devices can display. It can be a distraction from school work and also family life. There needs to be a policy for at home use as well as while being used at school.

The student needs to realise that the device is not theirs but the parents property and under their control while at home. This is always the case even if the device has been given as a gift for a birthday or Christmas. Also they need to understand that while the device is at school it is under the control of the school much the same way it is under the parent's authority at home.

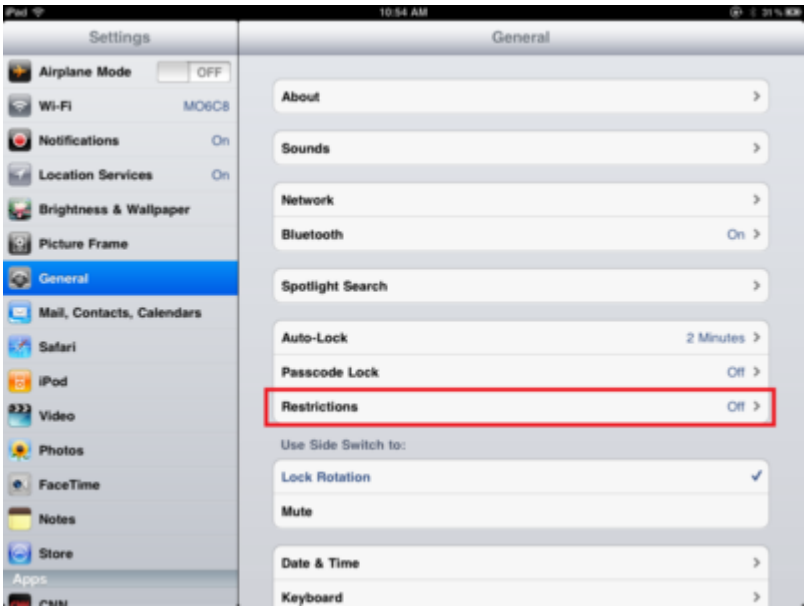
If you find that a child/student is having trouble handling the responsibilities of using a device then I recommend that the use of restrictions be applied to that device.

Restrictions can be used to limit what apps can be placed upon a device as well as what apps can be used at any time. This is done by setting restrictions and applying a pin number that restricts who has rights over an iPad.

This year the restrictions solution will be applied to any student iPad that misuses it during school time. All games and inappropriate apps will be wiped (this does not mean that paid apps are lost they just need to be reloaded at parent discretion) and a restriction code will be applied. Parents may receive this code from the school at any time or may place their own codes on if needed.

The following is how to place restriction if needed – these may be different or changed as new IOS standards are applied but can be found online.

## How to apply restrictions




The iPad's parental controls allow you to restrict how your child uses the iPad, from disabling the Safari browser to limit which websites your child can view to putting an age restriction on the apps downloaded. You can even turn off app downloads completely, which allows you to closely monitor what your child is doing on the iPad.

The iPad parental control works by setting a four digit passcode on the iPad that is required when setting the different restrictions. Once enabled, you can set restrictions for apps, television, music and movies.

### How to turn on parental controls for the iPad

The first step is to tap into the iPad settings by touching the settings icon. It looks like a bunch of gears and is one of the default icons for the iPad.

Once in settings, choose the general settings from the left-hand menu. You should reach a screen like the one shown above.

Next, choose Restrictions to enter the iPad settings for parental control.

The next step for enabling parental controls on the iPad is to turn on the iPad restrictions. Simply touch the top of the screen where it says **Enable Restrictions.**

You will be prompted for a four digit passcode. Choose something you will remember, but not something your child can guess like a birthday or the last digits of a driver's license. If there is a significant date you like to remember in your past besides birthdays and anniversaries that would be perfect.

The passcode for the iPad's restrictions will need to be entered twice to make sure you don't accidentally tap a different number than intended.

Once you have the iPad's parental controls enabled, you will be able to set different restrictions and even restrict some of the default applications that came with the iPad. This includes the Safari browser, YouTube and iTunes, so you can restrict your child's ability to view websites, watch videos and purchase music from their iPad.

You can also turn off the ability to install apps. You can still get apps on the iPad by installing them to iTunes and syncing them to the iPad, which will allow you to have complete control over which apps are on the iPad.

If you don't need that much control, you can set ratings restrictions for what type of apps can be installed on the iPad.

Another good thing to turn off is in-app purchases. Many free apps allow in-app purchases, which is how they make their money. This type of monetisation can be seen in apps like Pocket Legends, which is a great iPad app, but parents must be aware that it allows for the purchase of in-game money.

## Getting started and setting up an account

Before we begin to hand out apps for downloading you need to have an Apple ID and iTunes account. An appendix at the back of this manual shows over a number of pages how to create the account on your iPad. It is recommended that you use a username and password that is easy to remember as the student may need to tell the IT coordinator them if they need issues solved for them.

It is recommended that iTunes is downloaded on your computer at home to sync the iPad and computer for greater ease of transferring items between them. This is not necessary but can save a lot of issues in future.

You will be receiving a number of App codes and you may like to rewrite or stick them into this manual for later reference (a page example is provided)

## Redemption codes example sheet

This Sheet is to give you your redemption vouchers and also set out the basic guidelines to behaviour. See Appendix 2 **Redemption of iPad Vouchers** on how to use the codes

To understand how to use your redemption vouchers read the following - **Redemption Vouchers for Dummies sheets (see appendix)**

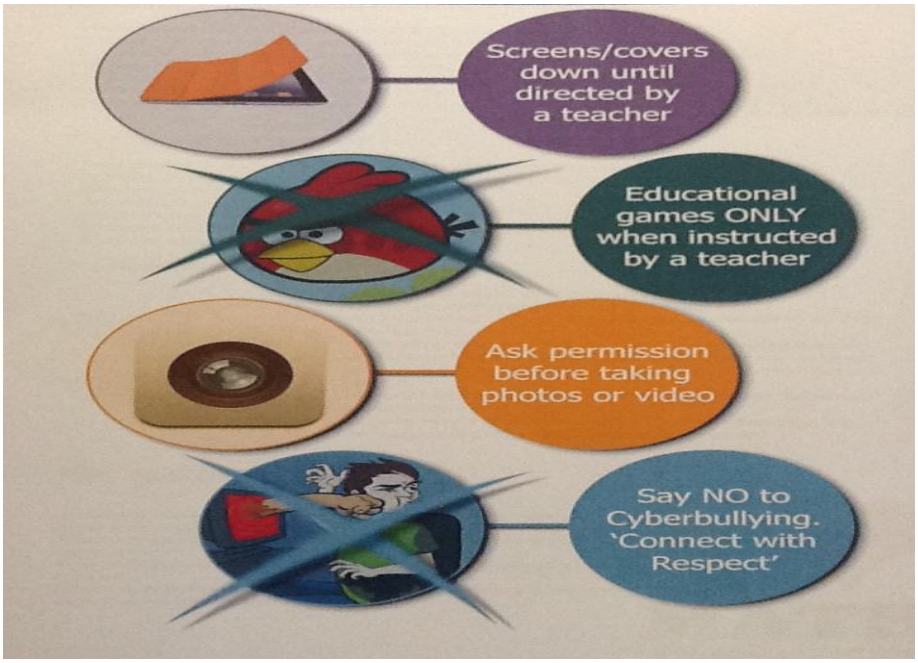
| Name of App | Voucher Code |
|---|---|
| Pages | |
| Keynote | |
| Numbers | |
| Notability | |
| imovie | |
| Garageband | |
| | |

## Computer Policy Handbook

The is included in the Appendix a St Pauls College Computer Policy Hand book as your student will come into contact and use computers during their schooling. Many of the policies cover the use iPad's in a number of ways like bullying, Internet usage, use of mobile devices and other areas so please have a look.

## Remember

1. Remember if a teacher asks for your iPad at any time don't argue just hand it over.
2. iPad's are not to be open at any time until your teacher asks you to use them
3. iPad's are not to be used outside of class time unless in the library
4. iPad's may be confiscated by teachers and student sent to Mr Westman


Screens/covers down until directed by a teacher
Educational games ONLY when instructed by a teacher
Ask permission before taking photos or video
Say NO to Cyberbullying. 'Connect with Respect'

**HAVE FUN BUT USE THE DEVICES IN SCHOOL AND AT HOME WITH RESPECT AND AS INTENDED BY TEACHERS AND PARENTS**

# APPENDIX

1. Creating an Apple ID/iTunes Account
2. Redemption of iPad vouchers
3. St Paul's College Netbook/Computer Acceptable Use Policy

# St Paul's College

# Student ICT

# Acceptable Use Policy

**St Paul's College Student ICT Acceptable Use Policy**

## 1. Policy Purpose

Computing devices and network access are provided to students to enhance teaching and learning. The use of these devices and services requires informed parental consent and appropriate management.

## 2. Background

Students, Teachers and other St Paul's College community members need to have clear guidelines to ensure that information technology resources are used appropriately. These guidelines will assist teachers at St Paul's College implement procedures that both protect and educate the students in their care.

## 3. Definitions

Computing Device – Includes Desktop computers, Laptop computers, Netbook computers, Tablet computers, mobile phones and other devices capable of accessing the College network.

Inappropriate Material – Any material that is offensive, abusive, discriminatory, defamatory, violent, illegal or lewd and lascivious (including, but not limited to, pornography) is considered inappropriate. If a student is unsure if material is appropriate they should check with their teacher before attempting to access it.

Bullying – Persistent and/or repeated behavior4 that is intended to cause hurt or distress to another person. Bullying may include, but is not limited to, social ostracism, repeated and persistent teasing and/or belittling, the sending of repeated harassing emails or text messages, the creation of websites design to defame or denigrate a person (including social media groups) or repeated harassment via Twitter.

## 4. Access and Security

Access to the College network is carefully monitored and controlled to safeguard student welfare and augment learning. Users are not to attempt to subvert the College network security systems, including, but not limited to, the College proxy server and installed anti-virus software.

Intentionally subverting these security measures may seriously compromise the safety and security of other users and will result in a loss of access privileges.

Any user who inadvertently discovers a breach of the College's security systems or who witnesses' inappropriate use of the College's network of computing devices is to report the incident immediately to their teacher.

## 5. Personal Information, Privacy and Confidentiality

College staff have to balance the privacy rights of individuals against their moral and legal obligation to protect students from harm and ensure that any computing resources are used to enhance teaching and learning. As such, teachers will inspect the contents of any computing device provided by the College from time to time. Furthermore, access to the Internet and the College network will be monitored and reviewed.

The College encourages Parents and Guardians to similarly monitor usage and access of the Netbook computers in the home.

## 6. Intellectual Property and Copyright

All users are expected to only use legal content on their College provided computing device. Using College resources to access illegal or pirated material is strictly prohibited and will result in a loss of access privileges. Further breaches may result in the matter being referred to the appropriate authorities.

Parents and students need to be aware that issues around intellectual property have not been fully

explored by our legal system. It is possible that schools, like Internet service providers, may be subject to legal action related to inappropriate use.

Furthermore, users are to ensure that any work that they submit or host on a College computing device or network is original and appropriately referenced. Plagiarism is a serious academic matter and may lead to disciplinary action.

## 7. Appropriate Use – Terms and Conditions

Students:

- agree to adhere to the terms and conditions set out in this *Acceptable Use Policy* each time they use a computing device provided by the College and/or access the College network.
- will ensure that all communication using the computing device provided by the College and/or separate online services is related to learning or school activities
- will keep passwords confidential, and change them when prompted or when known by another user
- will never knowingly allow others to use their computing device or network account unless directed to by a teacher for the purposes of collaborative learning
- will not send or publish unacceptable or unlawful material or remarks including offensive, abusive, defamatory or discriminatory comments
- will not access or attempt to access inappropriate material
- will not attempt to impersonate any other person when using the College provided computing device or College network
- will not engage in any bullying, intimidation or other inappropriate behaviour online
- will immediately tell a teacher if they receive a computer virus or a message that is inappropriate or makes them feel uncomfortable
- will never knowingly initiate or forward emails containing:
    - a message that was sent to them privately
    - a computer virus or attachments that are capable of damaging the recipients' computers
    - chain letters and hoax emails
    - "spam", like unsolicited advertising material, or mail unrelated to learning
- will not damage or disable computers, computer systems or networks of the College or other entity
- will not attempt any repairs on the computing device provided by the College, nor open the machine's enclosure in any way.
- will ensure that online services are not used for unauthorised commercial activities, political lobbying, gambling or any unlawful purpose.
- will not attempt to access the College's network using an unapproved private device, including but not limited to, smartphones or games devices
- will ensure that they have an appropriate data backup strategy. For example, all important data (e.g. assignments) should be backed up to an external device every week. Furthermore, important documents should also be stored in a "cloud-based" backup facility like Dropbox (www.dropbox.com).
- will not install software on any College computing device without completing the appropriate *Software Installation Request* document and receiving the approval of the Learning Technologies Coordinator.
- will promptly comply with all instructions from their teachers relating to the use of College computing devices and network systems.
- will ensure that any computing device is charged at night for use at school the following day.
- will not use any College computing device while travelling to and from the College or between classes. Any computing device must only be transported secured inside an appropriately padded bag.
- will not use any College computing device in the playground at recess or lunch.
- will complete regular cleaning and maintenance tasks as outlined in the *Netbook User Manual*.

- will not attempt to subvert any security measures installed on a College computing device including, but not limited to, removing pre-installed security software or installing alternative security software.
- will not install any games or unapproved entertainment software on a College computing device.
- will not use a College computing device to host, store, access or attempt to access any illegal or "pirate" content that the student is not able to prove that they legally own.
- Will not use any device to film or photograph at any time at school unless with teacher permission.

**Teachers**:

- are responsible for supervising student use of the College provided computing devices and access to the College network.
- are to maintain an informed view of the relative risks and educational benefits of online activity by their students. A variety of resources are available from the Inernet sites listed in Section 8 of this policy document.
- are to ensure that students are aware of the possible negative consequences of publishing identifying information online including their own or other students' images
- are to refrain from publishing student images or any student-identifying information on the Internet.
- are to check that any material planned for publication on the Internet or College network has the approval of the Principal and has appropriate copyright and privacy clearance
- are aware of the steps to take and advice to give if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public. Such steps may include:
  - collecting as much information as possible about the incident including copies of communications
  - emphasising to the student that the event is not necessarily their fault
  - identifying any risky behaviours on the part of the reporting student and counseling them on the need to adopt more protective behaviours
  - if the incident warrants further attention inform the Principal of the incident (for example, if the teacher suspects the student may have been placed in a position of harm).
- are to inform parents that student Internet access from home or other non-school sites does not occur via the College's network and therefore Internet browsing may not be filtered
- should promote the use of strong passwords for students who can cope with the complexity. Stronger passwords:
  - contain a mixture of alphabetic and non-alphabetic characters
  - are changed frequently
  - do not contain dictionary words
  - do not contain easily identified personal information such as name, date of birth, etc.
  - do not contain any part of the account identifier such as the username
  - are not written down.

## 8. Online resources for Appropriate Usage and Cyber-Safety

http://www.cybersmart.gov.au/
http://www.theline.gov.au/

---

I have read and agree to abide by the conditions of use as outlined in the ICT Acceptable Use Policy.

Student's Name :..... PC Class:.....….

Student's Signature :..... Date:.....

Parent's Signature :..... Date:.....

# St Paul's College: iPad Pledge

1. I will keep the iPad in my possession, unless it is locked in my locker.
2. I will never loan the iPad to other individuals.
3. I will arrive at school with the iPad fully charged every day.
4. I will protect my iPad by keeping it in a protective cover.
5. I will not change or remove profile settings on the iPad.
6. I understand that the iPad is subject to inspection at any time.
7. I will hand my iPad to a teacher on demand and supply the password if necessary.
8. I will only use my Apple ID on the iPad. **Do not allow friends to use your Apple ID.**
9. I will not handle another student's iPad without their permission.
10. I will follow the St Paul's College Kempsey Responsible Use Agreement.
11. I will use the school Internet resources for educational purposes only.
12. I will file a police report immediately if the iPad is stolen, and tell school about it.
13. I am responsible for damage caused by neglect or abuse.
14. I understand that the iPad is an educational tool which is available to my parents/carers at all times. I will make it available to them on request.
15. I will not use the camera or video on my iPad without teacher permission
16. I have the option to purchase insurance and I am responsible for all costs personally.

**iPad Management:**

1. School purchased apps will be given out to students and expected to loaded on iPads
2. Each user or user's parent must create a personal iTunes account to "purchase" personal apps, free school-related apps, and iBooks. **A credit card is not required to set up an iTunes account.**
3. Personalised apps such as games are not to be used at school without permission.
4. iPads may be confiscated and held at the school if misused, until disciplinary action is undertaken or parents contacted to collect device.
5. At home use is at the discretion of parents and their rules.

I have read the STUDENT iPad Pledge and understand that I am responsible at all times for the care and appropriate use of technology. I understand if I violate the guidelines agreed to in the St Pauls College Computer Policy Handbook, my privilege to use technology may be restricted or removed, and I may be subject to disciplinary action.

_____

Parent Signature Date

_____

Student Signature Date

# COLLEGE COPY

## St Paul's College Student ICT Acceptable Use Policy

I have read and agree to abide by the conditions of use as outlined in the ICT Acceptable Use Policy.

Student's Name :..... PC Class:.....….

Student's Signature :..... Date:.....

Parent's Signature :..... Date:.....

---

## St Paul's College: iPad Pledge

I have read the STUDENT iPad Pledge and understand that I am responsible at all times for the care and appropriate use of technology. I understand if I violate the guidelines agreed to in the St Pauls College Computer Policy Handbook, my privilege to use technology may be restricted or removed, and I may be subject to disciplinary action.

_____

Parent Signature Date

_____

Student Signature Date